AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims, in which claims 3, 18, 32, 47 and 61 are currently amended.

1. (Canceled)

2. (Canceled)

3. (Currently Amended) A network apparatus, comprising:

a proxy which facilitates communication with other network entities by performing at least one performance enhancing function, the proxy communicating with the other network entities via a first type of connection and a second type of connection,

wherein the proxy establishes multiple connections of the first type associated with different applications, and includes

a spoofing element configured to intercept and alter a data flow within one of the connections to add to or delete from the data flow to reduce startup latency, ~~which~~ the spoofing element only ~~spoofs~~ spoofing connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired.

4. (Canceled)

5. (Original) The network apparatus of claim 3, wherein said spoofing element assigns spoofing resources, including buffer space and control blocks, to the spoofed connections.

6. (Original) The network apparatus of claim 3, wherein said spoofing element spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

7. (Original) The network apparatus of claim 6, wherein said spoofing element defines the at least one spoofing rule in a spoofing profile.

8. (Previously Presented) The network apparatus of claim 3, wherein the spoofing element spoofs acknowledgements (ACKs).

9. (Previously Presented) The network apparatus of claim 3, wherein the spoofing element spoofs a three-way handshake between said network apparatus and another network entity.

10. (Previously Presented) The network apparatus of claim 3, wherein the proxy includes a protocol element, which multiplexes multiple connections of the first type onto a single connection of the second type.

11. (Previously Presented) The network apparatus of claim 3, wherein the proxy includes a prioritization element, which prioritizes connections of the first type to determine what priority level of the connection of the second type, each of the connections of the first type are assigned.

12. (Original) The network apparatus of claim 11, wherein said prioritizing element prioritizes connections using at least one prioritizing rule based on destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field, a type of data contained within the connection or combinations thereof.

13. (Original) The network apparatus of claim 12, wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile.

14. (Previously Presented) The network apparatus of claim 3, wherein the proxy includes a path selection element, which selects a path for data associated with connections of the first type across connections of the second type or connections of other types.

15. (Original) The network apparatus of claim 14, wherein said path selection element can select up to N paths (N>1), where the Nth path is selected only if the (N-1)th path fails.

16. (Original) The network apparatus of claim 15, wherein said path selection element selects a path using at least one path selection rule based on priority, a destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field or combinations thereof.

17. (Original) The network apparatus of claim 16, wherein said path selection element defines the at least one path selection rule in a path selection profile.

18. (Currently Amended) The network apparatus of claim 3, wherein the proxy includes a compression~~/~~ and encryption element, which compresses and~~/or~~ encrypts data associated with connections of the first type for transmission across connections of the second type.

19. (Previously Presented) The network apparatus of claim 3, wherein the first connection uses a high layer protocol.

20. (Previously Presented) The network apparatus of claim 3, wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

21. (Previously Presented) The network apparatus of claim 3, wherein the second connection is a backbone connection.

22. (Previously Presented) The network apparatus of claim 3, wherein the backbone connection is via a wireless link.

23. (Original) The network apparatus of claim 22, wherein the wireless link has high latency and high error rate.

24. (Original) The network apparatus of claim 22, wherein the wireless link is a satellite link.

25. (Previously Presented) The network apparatus of claim 3, wherein said network apparatus is a component of a network gateway.

26. (Previously Presented) The network apparatus of claim 3, wherein said network apparatus is a component of a host.

27. (Previously Presented) The network apparatus of claim 3, wherein said network apparatus is a component of a hub.

28. (Previously Presented) The network apparatus of claim 3, wherein said network apparatus is a component of a VSAT.

29. (Previously Presented) The network apparatus of claim 3, wherein said network apparatus is a component of a router.

30. (Canceled)

31. (Canceled)

32. (Currently Amended) A method for providing data communication with a plurality of network entities, comprising:

facilitating communication with the network entities by performing at least one performance enhancing function;

communicating with the network entities via a first type of connection and a second type of connection;

establishing multiple connections of the first type associated with different applications; ~~and~~

intercepting and altering a data flow within one of the connections to add to or delete from the data flow to reduce startup latency; and

spoofing only connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired.

33. (Canceled)

34. (Original) The method of claim 32, wherein said spoofing step assigns spoofing resources, including buffer space and control blocks, to the spoofed connections.

35. (Original) The method of claim 32, wherein said spoofing step spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

36. (Original) The method of claim 35, wherein said spoofing step defines the at least one spoofing rule in a spoofing profile.

37. (Previously Presented) The method of claim 32, further comprising:

spoofing acknowledgements (ACKs).

38. (Previously Presented) The method of claim 32, further comprising:

spoofing a three-way handshake another network entity.

39. (Previously Presented) The method of claim 32, further comprising:

multiplexing multiple connections of the first type onto a single connection of the second type.

40. (Previously Presented) The method of claim 32, further comprising:

prioritizing connections of the first type to determine what priority level of the connection of the second type, each of the connections of the first type are assigned.

41. (Original) The method of claim 40, wherein said prioritizing step prioritizes connections using at least one priority rule based on destination address, source

address, destination port number, source port number, protocol, a differentiated services (DS) field, type of data contained within the connection or combinations thereof.

42. (Original) The network apparatus of claim 41, wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile.

43. (Previously Presented) The method of claim 32, further comprising:

selecting a path for data associated with connections of the first type across connections of the second type or connections of other types.

44. (Original) The method of claim 43, wherein said selection step selects up to N paths (N>1), where the Nth path is selected only if the (N-1)th path fails.

45. (Original) The method of claim 44, wherein said selection step selects a path using at least one path selection rule based on priority, a destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field or combinations thereof.

46. (Original) The method of claim 45, wherein said selection step defines the at least one path selection rule in a path selection profile.

47. (Currently Amended) The method of claim 32, further comprising:

compressing and~~/or~~ encrypting data associated with connections of the first type for transmission across connections of the second type.

48. (Previously Presented) The method of claim 32, wherein the first connection uses a high layer protocol.

49. (Previously Presented) The method of claim 32, wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

50. (Previously Presented) The method of claim 32, wherein the second connection is a backbone connection.

51. (Original) The method of claim 50, wherein the backbone connection is via a wireless link.

52. (Previously Presented) The method of claim 32, wherein the wireless link has high latency and high error rate.

53. (Previously Presented) The method of claim 32, wherein the wireless link is a satellite link.

54. (Previously Presented) The method of claim 32, wherein said method is performed in a network gateway.

55. (Previously Presented) The method of claim 32, wherein said method is performed in a host.

56. (Previously Presented) The method of claim 32, wherein said method is performed in a hub.

57. (Previously Presented) The method of claim 32, wherein said method is performed in a VSAT.

58. (Previously Presented) The method of claim 32, wherein said method is performed in a router.

59. (Previously Presented) The method of claim 32, wherein said method is performed in a switch.

60. (Canceled)

61. (Currently Amended) A method for providing data communication over a satellite network, the method comprising:

communicating with a plurality of hosts over a plurality of connections corresponding to a plurality of applications resident on the respective hosts;

determining which of the plurality of connections, according to the respective applications, is to receive priority processing for transport over a backbone connection established over the satellite network;

encrypting and compressing data streams associated with the priority connections based on a transmission constraint of the backbone connection; and

transmitting the encrypted and compressed data streams over the backbone connection, and concurrently acknowledging the corresponding hosts.

62. (Previously Presented) A computer-readable medium bearing instructions for providing data communication over a satellite network, said instruction, being arranged, upon execution, to cause one or more processors to perform the method of claim 61.